

REMARKS

Claims 1-19 were presented for examination.

Claims 1-19 were rejected.

Applicant is hereby amending claims 1, 3, 5, 8, 10-13, 16, and 18-19; and canceling claim 9; all of the foregoing merely to distinctly claim their invention. Claims 1, 18, and 19 have been amended merely to incorporate the limitations of claim 9, to correct minor typographical errors and for proper antecedent bases. Except as noted below for claim 3, all other amended claims have been amended merely to correct minor typographical errors and for proper antecedent bases.

Reconsideration of this application as amended, and allowance of all pending claims, claims 1-8 and 10-19 as amended, is hereby respectfully requested.

Title

As requested in the Office Action, Applicant is replacing the title with one that is more clearly indicative of the invention to which the claims are directed.

Claim 3, under 35 U.S.C. § 112, second paragraph

Claim 3 was rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Specifically, the Office Action objects to the use of the term “bona fides.”

Applicant is amending claim 3 to replace “bona fides” with “authentication data.” This term is used in the specification and the amendment is supported, for example, by FIG. 2 et seq.

Applicant submits that claim 3 as amended now defines the invention with sufficient particularity

and distinctiveness to be patentable to Applicant and requests withdrawal of the rejection made under § 112.

Claims 1, 5-8, 16-19 under 35 U.S.C. § 102(e) in light of Fielder, and claims 2-4 under 35 U.S.C. § 103(a) over Fielder in view of Yatsukawa

In paragraphs 9-24 of the Office Action, claims 1-8 and 16-19 were rejected variously in light of Fielder, or in light of Fielder in combination with Yatsukawa. Applicant is amending the three independent claims (claims 1, 18 and 19) to include the limitations of the original claim 9. Since the rejections in light of Fielder and Fielder/Yatsukawa were not applied to the original claim 9, Applicant respectfully submits that claims 1, 18 and 19, as amended, are patentably distinguishable over the cited references.

Claims 9, 11-12, and 14-15 under 35 U.S.C. § 103(a) over Fielder in view of Menezes; and claims 10 and 13 under 35 U.S.C. § 103(a) over Fielder in view of Menezes and Lamport

In paragraphs 25-30 of the Office Action, claims 9-15 (all of which originally depended from claim 9) have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Fielder in view of Menezes, in some cases in further combination with Lamport. These rejections are respectfully traversed.

The original claim 9 expressly recites that update data is sent from the server device to the client device. In direct contrast, Fielder expressly states that no update data is sent between devices. Even if Menezes teaches sending update data from one device to another, it cannot be properly combined with Fielder since the combination would change both the principle of operation and the intended function of Fielder.

The following more detailed remarks will be made with respect to independent claims 1, 18, and 19, since these independent claims are amended to include the limitations of the original claim 9.

Taking claim 1 as an example, claim 1 concerns validating a client device by a server device through use of a shared unpredictable secret. One step involves replacing the shared unpredictable secret. Specifically,

“the server device sends update data to the client device;
the client device applies the update data to the shared unpredictable secret to
generate a new secret; and
the client device replaces the shared unpredictable secret with the new secret.”

Claim 1 expressly recites that the server device sends update data to the client device. This feature is beneficial because it allows a client device to generate a new secret based on update data sent by the server device.

The rejections in the Office Action are based on a combination of Fielder and Menezes. The Office Action states that Fielder discloses the originating system (the alleged “client device”) applying a change value (the alleged “update data”) to the dynamic secret in order to update the secret, but fails to disclose the change value being received from the answering system (the alleged “server device”). The Office Action then goes on to state that Menezes discloses sending update data between devices and, therefore, the original claim 9 was rejected in light of the combination of Fielder and Menezes.

Regardless of whether the combination teaches all the elements of the original claim 9, the combination of Fielder and Menezes itself is not proper. One of the advantages of Fielder’s system is that the change value (the “update data”) is expressly not sent from one device to the other, thus preventing discovery of the change value during the sending. Fielder expressly states

that “. . . the change value is not made part of any access request or information that is exchanged between the computer systems. Thus, the change value is not subject to discovery as a result of information communicated over the communication link 12.” Col. 6 line 58 – col. 7 line 3. Furthermore, the originating and answering systems generate “. . . the same passwords, secret session encryption key, and change value without exchanging more than an access request and their respective system identifiers . . .” Col. 10 lines 24-27. In other words, the devices each independently generate the change value; the change value is not sent between devices.

Since Fielder expressly states that the change value is not sent between devices, Fielder cannot be properly combined with a reference that teaches exactly the opposite. It is well established that a combination of prior art is improper if the combination would change the principle of operation of a reference. M.P.E.P. § 2143.01, citing *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959). In this case, the alleged combination of Fielder and Menezes would require sending the change value between Fielder’s computer systems, which would change Fielder’s basic principle that no change value is sent between the computer systems. Similarly, references are not properly combinable if their intended function is destroyed. M.P.E.P. § 2143.01, citing *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). In this case, the alleged combination would destroy Fielder’s intended function of communication without exchanging the change value.

It is therefore respectfully submitted that independent claim 1, as amended, is patentably distinguishable over the cited references. Independent claims 18 and 19 have the same limitations and are patentably distinguishable for the same reasons. Dependent claims 2-8 and 10-17, as amended, all depend from claim 1, and are therefore allowable for the same reasons.

Closing

Applicant believes that the application is in condition for allowance of all claims herein, claims 1-8 and 10-19 as amended, and therefore an early Notice of Allowance is respectfully requested. If the Examiner believes that for any reason direct contact with Applicant's attorney would help advance the prosecution of this case to finality, the Examiner is invited to telephone the undersigned at the number given below.

Respectfully submitted,

WARWICK FORD

Date: MAY 11, 2005

By: 

Michael W. Farn
Attorney for Applicant
Registration No. 41,015

Fenwick & West LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
(650) 335-7823 (Tel)
(650) 938-5200 (Fax)